OIT 0810-86
16 SEP 1986

MEMORANDUM FOR: Chief, Evaluation and Plans Staff, DO

FROM: Edward J. Maloney
Director of Information Technology, DA

25X1 SUBJECT: Proposal for Computer Security Library [redacted]

REFERENCE: Your memo, Same Subject, dtd 9 Sept 1986, w/atts

1. In the reference, you asked for this Office's views on the establishment of a Computer Security Library in IMS. Due to the very short deadline, we have had time only to review the attachments to the reference. Based on this review, we believe that there are higher priority tasks that could be addressed with the proposed funding. In the tight funding situation that the Agency will be facing in FY 1987 and beyond, we will have to make very difficult resource decisions. Instead of the proposed library, there are pressing computer security problem areas, such as auditing, access controls, encryption, labelling, etc. where the proposed $292K in funding could bring us some very positive benefits in terms of research and development and implementation
25X1 of sorely needed systems and software. [redacted]

2. In addition to the low priority we would assign this task, we are concerned there are hidden costs that have not been addressed in the IMS proposal. The impact of the final system on processing resources should be assessed before a commitment is made to this project. It is probable that this library system would require considerable processing power and direct access storage, as well as system programming and operations support. We are concerned that IMS would look to OIT to provide these unprogrammed resources. The library system may have security implications as well. In order for other components, such as ISSD/OS, to have access to the data base, connectivity would have
25X1 to established for DO users with the [redacted] Center, or for ISSD/OS users with the Special Center. Both solutions have their own set of costs and potentially significant security problems.

25X1 [redacted]

25X1 [redacted]

SECRET

25X1 SUBJECT: Proposal for Computer Security Library [redacted]

3. The Office of Information Technology is second to none in this Agency in our concern for computer security. We pride ourselves in our specialized systems expertise. We have made extensive use of this expertise in ensuring that the Agency network is as secure as both technology and resources will allow. Our auditing activity, for example, has had an outstanding record of success in identifying threats to the security of Agency information. Our active program in computer security naturally requires access to the current literature. We, however, do not view obtaining this access as a major problem. Much of the information described in the reference is available through such sources as the National Technical Information Service (a Department of Commerce activity), which routinely publishes extensive bibliographies on computer security, or outside data bases available through the Agency Library (e.g., NEXIS, DIALOG). In terms of priorities, the Computer Security Working Group of the Agency's Information Systems Board two years ago did an in-depth study of key problems in the computer security area. Lack of access to the literature was not mentioned. There were, however, approximately a dozen areas that were in need of our attention and funding. Anyone of those areas would benefit greatly from the funding planned for the library project. [redacted] 25X1

4. Should this project be initiated, we recommend, under the circumstances, that a reduced amount of funding be allocated. These funds should be used to investigate the requirement, including the availability of alternate means of accessing the required information; and lifecycle costs, including the hardware, software and support implications. The results of this preliminary study should be carefully reviewed before a decision is made to proceed with full funding. [redacted] 25X1

5. Due to time constraints, we have not been able to fully assess the IMS proposal. Whatever your directorate's decision on this project, this Office stands ready to assist in a more detailed evaluation. Should you wish to convene a task force or study group, please do not hesitate to contact me or, my deputy, 25X1 [redacted] Computer security is an area of such importance and complexity that all involved Agency components must work closely together. Thank you very much for your concern and allowing us to comment on this proposal. [redacted] 25X1

/S/

Edward J. Maloney

25X1

Attachment:
Reference

MD/OIT/[redacted] (15Sep86)
Distribution:
Original 1 - Addressee
1 - MD Chrono 1 - MD Subject
1 - OIT/FO 2 - OIT Registry

9 SEP 1986

MEMORANDUM FOR: Chief, Office of Information Technology

25X1

FROM: [redacted]
Chief, Evaluation and Plans Staff

SUBJECT: Proposal for Computer Security Library

REFERENCES:
A. DO/IMS 86-047/3
B. EPS memorandum, 14 August, Same Subject
C. DO/IMS 86-047/2

1. The Evaluation and Plans Staff requests your views regarding the Reference A proposal. To assist you in this effort, the following background may be helpful: Reference C, prepared by the Information Management Staff of the Directorate of Operations, requested DDO approval for entering into negotiations with a private firm (ETI) for the production of an automated computer security library. Reference B, prepared by EPS, informed IMS of important issues which should be addressed before EPS could forward the proposal to the DDO for consideration,

2. Reference C therefore represents the IMS response to the questions posed by EPS. Now that we have the response in hand, we believe (as stated in the paragraph 3 of the EPS memo) that formal OIT coordination should be obtained before we make our final determination regarding the merits of the program. Specifically, we would appreciate OIT views concerning the IMS response to each of the generic issues (operation, development, management) raised in the attached memoranda. We would also appreciate your overall evaluation of the usefulness such a program; i.e., is this type of information/data available from other sources; could such a capability be created through "in house" elements, without negotiating with outside contractors? Thank you very much for your assessment. We realize this is a relatively short time frame in which to reply, but we would greatly appreciate your response by Close of Business on Friday, 12 September.

25X1

[redacted]

Action to C/19 + CG

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Information Management Staff's Response to Concerns Raised Against the Proposed Computer Security Library

STAT FROM: [redacted] STAT C/IMS 1D4109 Hqs	EXTENSION [redacted]	NO.	DATE 2 August 1986

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. C/OIT 2D02 Hqs				The attached is a copy of our response to OIT's concerns raised and incorporated in AC/EPS' memo of 14 Aug 1986 concerning our proposal for a computer security library. We have obtained coordination from C/ISSD/OS and C/CI/T. We have resubmitted our request to negotiate a contract for feasibility and proof of concept. We look forward to your assistance and cooperation in this effort
2.				
3.				
4.				
5.				
6.				Ed / Leo We originally ~~said~~ the [illegible] [illegible] a waste of $250K. Value added to computer security would be slight. They're charging on ~~[illegible]~~ their money. We don't want it in
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				STAT [redacted] Center &
15.				bet. How/who

do you (want to)

FORM 610 USE PREVIOUS

DO/IMS 86-047/3

3 SEP 1986

MEMORANDUM FOR: Acting Chief, Evaluation and Plans Staff

25X1 FROM: [redacted]
Chief, Information Management Staff

SUBJECT: Information Management Staff's Response to Concerns Raised Against the Proposed Computer Security Library.

REFERENCE: Your Memorandum, dated 14 Aug 86, Same Subject

1. In response to concerns raised within your memorandum concerning our proposal for the development of a Computer Security Library, we are submitting the following which are keyed to your memo's format:

Operation:

25X1 A Computer Security Library is required primarily for the [redacted] within the Directorate of Operation's Information Management Staff (IMS). Its availability to other Agency elements is offered as a secondary service, according to their independent as well as shared computer security requirements. Location of the Library within the Special Center was not previously specified. On the contrary, because it was envisioned as a resource which could be shared in the future, initial thinking placed the Library in the [redacted] Center. Regardless of its placement, "whether and how" would be the outcome of the contractor's requested tasking related to "feasibility and proof of concept". 25X1

25X1 A position within [redacted] IMS has been designated to fulfill the functions of the data base administrator.

25X1 [redacted]

Per paragraph two of the Request For Approval To Negotiate, the contractor would be tasked to "develop procedures for periodic updating of the library content." The cost is currently estimated to be less than the initial start-up costs.

Development:

The contractor has an established reputation for developing and managing all phases of library operations (previous contracts with the Department of Energy, Department of Education, NASA, AID, ACTION, FEMA).

The selection of a data base management system is governed by end user requirements for storing and retrieving information. Thus, the selection of a specific system such as SQL, ADABAS, MODEL 204, IDMS, etc., would be premature at this time but would be determined during the "feasibility proof of concept" phase. It is our understanding that a query language is associated with all major data base management systems.

The proposed contractor has a Computer Technology Division which is skilled in the use of data base management systems and query languages in a broad variety of applications, including library sciences.

The estimated costs for the first and succeeding years has been given careful consideration by IMS and have been found to be commensurate with the priority of the requirement.

Management:

We believe the end product (feasibility and proof of concept) resulting from the initial contract will provide a sound basis for either launching, redesigning, or abandoning the implementation phase.

2. The priority requirement for a Computer Security Library can best be understood in light of the establishment and mission of [redacted] was established in March 1985, in the wake of growing concern within the Directorate for improving the security of ADP

25X1

25X1 systems under the Directorate's control. [redacted] was charged with ensuring the security of the DO's ADP systems in a way that provides an optimum balance between security and production. 25X1 Thus, [redacted] was tasked to:

- advise DO management concerning the weaknesses and vulnerabilities in its computer security posture and plans, and identify and resolve the gaps and constraints which result from adherence to existing and future computer security policy and regulations;

- maintain knowledge of computer security research and technology, computer security policy and regulations, and computer security in general as a basis for recommending solutions to current and future computer security problems;

- provide comprehensive assessments and independent judgments (the substance of which can be keyed to the content of the proposed library) to increase the confidence level of DO decisions and maintain Directorate integrity, ie. need to know.

25X1 After one year of existence as a staff, [redacted] has found that the methods of obtaining, storing, recalling, and sharing needed information as referenced in paragraph 2 are at best ad hoc and certainly not comprehensive. We have found that the nature of these external contacts and relationships do not automatically nor 25X1 should they necessarily serve the total interest of IMS. [redacted] was created to carry the DO's computer security portfolio and, thereby, capture, organize and systematically disseminate needed computer security information to DO managers.

With the proposed library we ensure that:

- The assessments and judgments given are based on current knowledge and a comprehensive search (internally and externally) of readily available information.

- The response to a first query concerning capability and vulnerability can be readily recalled in response to a similar second query and that currently scattered knowledge becomes more centrally located.

- Current and ongoing computer security within the DO will have the benefit of the research and application going on in private industry as well as the knowledge and experience of the past.

- ISS will independently maintain up-to-date knowledge of computer security law, abuse, and training.

- Comprehensive computer security information is available in an accessible mode for retrieval by pertinent computer security components.

25X1

[redacted]

4 JUL 1986

MEMORANDUM FOR: Chief, Information Management Staff

25X1

FROM: [redacted]
Acting Chief, Evaluation and Plans Staff

SUBJECT: Proposal for Negotiating Contract with Private Firm for Development of Computer Security Library

REFERENCE: DO/IMS 86-047/1

1. Several important issues concerning the operation, development and management of the proposed computer security library must be addressed before the referenced memorandum can be forwarded to the DDO and before any consideration can be given to negotiating a contract for this project.

OPERATION:

--If this is indeed an Agency-wide, rather than a DO system, we must address whether and how it would be connected to the Special Center.

--The Data Base Administrator functions need to be clearly defined.

--A major problem would be in keeping the data base up-to-date. Who and how are big questions, not to mention the cost of keeping it current and usable.

DEVELOPMENT

--The basic functions of a library (storage or articles and periodicals; indexing by title, subject and author; and retrieval) are fairly well understood and can be satisfied by a data base management system such as System Query Language (SQL).

--The creation of specialized interest files and the dissemination of articles based upon interest is more complex, however, and needs a "proof of operations" concept up front. (These functions are provided by systems such as

25X1

[redacted]

SAFE Delivery 2 and the Department of Justice product known as JURIS.)

--The creation of the data base is also a major cost item.

MANAGEMENT

--If such an effort is undertaken, a proof of operations concept, as stated above, is necessary and makes a lot of sense.

2. Information security specialists within the Office of Security (OS/ISSD) regularly receive a "bulletin-board" service from the National Computer Security Center, listing the most up-to-date publications in this field and providing other details as to who and what companies are doing different types of work regarding computer security. OIT also has access to this information. OIT and ISSD regularly send officers to seminars and conferences to obtain the most up-to-date information regarding work in this field. The Agency also benefits from information on this subject which it receives from its IBM contractors. OIT and ISSD officers state that while a centralized library might be "nice to have," it certainly is not necessary; furthermore, because developments in this field are so fast-moving, any library we create could become obsolete very quickly.

3. With the above in mind, therefore, EPS does not recommend forwarding this request to the DDO at this time. If IMS desires to pursue this proposal, we suggest that you address the above-cited issues via separate correspondence, to be sent to Chief/EPS via Chief/OS/ISSD and Chief/OIT as well as CI/T.

25X1

[redacted]

SECRET

DC/IMS 86-0471

21 JUL 1986

MEMORANDUM FOR: Deputy Director for Operations

VIA: Chief, Evaluation and Plans Staff

25X1 FROM: [redacted]
Chief, Information Management Staff

SUBJECT: Request for approval to negotiate contract with Evaluation Technologies, Inc. for development of an Automated Computer Security Library

ACTION REQUESTED

1. Your approval is requested to enter negotiations with Evaluation Technologies, Inc. for the production of an Automated 25X1 Computer Security Library. The library will enable [redacted] 25X1 [redacted] and other information security elements within the Agency to make a comprehensive survey of what is being done in computer research and what is available in the way of computer security software and hardware.

2. For an estimated first year cost of $292K, the contractor will deliver an automated library based on user requirements; provide ongoing access to hard copy literature; provide an alert process for timely dissemination of information relevant to current issues; and develop procedures for periodic updating of the library content. The initial funds requested for FY 86, $50K will enable the contractor to determine feasibility and proof of concept.

3. The Automated Computer Security Library will service 25X1 IMS [redacted] the Information Systems Security Division of OS (OS/ISSD), and portions (Computer Security Policies, Regulations and Procedures) will be available to managers and other users.

25X1

25X1 [redacted]

SECRET

[redacted]

25X1 The library will enable IMS [redacted] as well as OS/ISSD to make better judgments concerning the introduction of computer security technology; develop recommendations to reduce or eliminate vulnerabilities and potential threats posed by the introduction of new computer technology; and thus, improve the security of information systems serving the DO and the Agency. The automated library will include an unclassified section and a classified section; be housed within an Agency mainframe; with special access by computer security specialists and other designated users. The content of the library will include computer security literature, terminology, products (capabilities, vulnerabilities and countermeasures), research, policy and regulations, law, abuse cases, training, companies and personalities.

BACKGROUND

4. IMS has been directed to ensure the security of computers and word processors which service the Directorate's information requirements. This requires making judgments on the security aspects of new and current technology; recommending security techniques for current and future use; seeking solutions to unique Directorate problems, such as compartmentation; and,contributing to long-range planning efforts, such as Project George and ALLSTAR UPGRADE. Computer security technology, which includes vulnerability and risk assessment, authentication, auditing, contingency planning, and damage recovery responsibilities, is currently outpaced by computer technology. As computer capabilities increase, so do the problems of compartmentation, authentication and auditing. Related to these problems is the need to protect all systems from electronic penetration. We anticipate that our ability to review new computer security products and techniques will be overtaken by the growth in computer security science and technology within private industry, which is being stimulated by the requirements NSA is imposing and the growing national concern about computer crime. On the one hand, we must protect the current environment. On the other, possible vulnerabilities associated with planned upgrades must be assessed, and it is important to recognize when new technology can pose a threat to currently installed safeguards.

JUSTIFICATION

5. There is an ongoing need to provide comprehensive advice and apply sound judgment to the introduction of new automated data

processing systems in the areas of clandestine operations and Directorate information systems. Our responses to requirements have been limited by our lack of ready access to available information. Responses to agent, NOC, and Station requests to use off the shelf equipment could be enhanced by providing comprehensive vulnerability assessments along with suggested security countermeasures. Recommendations made by the DO's Information Security Task Force could be addressed in a more comprehensive and timely fashion. Confidence in plans for deploying PCs and Optical Character Readers in a compartmented environment in Conus and overseas could be increased with broader knowledge of vulnerabilities and countermeasures. Without the proposed capability, we will be circumscribed to continue to rely on sporadic bits and pieces of information and home-grown solutions.

6. The Agency's Information Systems Board has "resolved to stop depending on costly home-grown solutions for our information technology needs. We intend to rely on solutions that have won general acceptance throughout the communication and data processing industry. The decision to move into the IBM 3270-compatible world is an important example."

25X1 7. Current program priorities and staffing levels of IMS [redacted] and OS/ISSD do not permit the time and person resources required to keep us informed, in a comprehensive way, of those solutions which are available and may have "won general acceptance throughout the data processing industry."

8. The mechanism of a contractor has been chosen because it provides the Directorate and the Agency with a reasonably immediate, reliable and low profile capability for meeting a high priority requirement for extracting information and knowledge from the private sector. It provides the flexibility for expansion to meet associated requirements or contraction to meet maintenance and updating requirements once the library has been established.

9. ETI has been selected based on its submission of an unsolicited proposal of which the "library" was one element, based on its expertise in the development of automated libraries and knowledge transfer methods, and based on the qualifications of Mr. Ron Turner, Chief Marketing Officer for ETI and the proposed project director. He has 30 years of computer and business experience in the field of computer security. We have selected the sole source route for security reasons: the Directorate's computer capabilities and vulnerabilities should not be exposed to the open bidding process, in view of the fact that computer contractors are prime targets of the opposition. Limiting the contract to ETI, a certified 8a minority contractor with an

impressive record of service to Government and private enterprise, will minimize the risk of exposing Agency methods and capabilites, as well as advance the Agency's and Directorate's desire to award contracts to minority-owned businesses.

FUNDING

10. Because of the late starting schedule, the FY 86 program is not expected to exceed $50,000. These funds will enable ETI to determine feasibility and proof of concept based on the user's content and format requirements, availabe sources of material, the proposed automated system, ETI's methods and experience, the user's service delivery requirements, and the user's acquisition procedures. IMS will attempt to reprogram FY 86 and FY 87 funds for this priority requirement.

COORDINATION

11. The content of the proposed library is the result of numerous discussions between IMS [redacted] and OS/ISSD. Although it will meet the independent needs of both ISS and ISSD, it also, in many ways, will enable and encourage cooperative use.

[redacted]

Attachments:
- A. Description
- B. Statement of Work

SUBJECT: Request for approval to negotiate contract with Evaluation Technologies, Inc. for development of an Automated Computer Security Library

CONCUR:

Chief, Evaluation and Plans Staff ____________ Date

APPROVED:

Deputy Director for Operations ____________ Date

ATTACHMENT A

DESCRIPTION

The Automated Computer Security Library will include the following elements:

- Computer security publications, articles (index and hard copy);
- Computer security terms, concepts, glossary;
- Computer security products -(summary features of hardware and software, state of the art systems, commercial capability assessments, and vulnerability assessments);
- Computer security research;
- Computer security policy and regulations;
- Computer security law;
- Computer security abuse cases;
- Computer security training courses, seminars, symposiums, conferences;
- Companies specializing in computer security;
- Who's who in computer security.

ATTACHMENT B

STATEMENT OF WORK

The primary purpose in hiring ETI is to keep pace with computer security science and technology by capturing and transforming the bulk of available knowledge and information to a readily accessible form and in a manner which ensures timely dissemination and use. Within the first three months, ETI will:

- develop plans and procedures for the automated computer security library;
- identify information sources (literature, publications, info banks, clearinghouses);
- define procedures for information receiving, processing, review and analysis, automating, and updating (ETI staff work);
- determine user retrieval needs (format, quantity, frequency);
- define service methods (hard copy, automated data base access, alert mechanism, updating process);
- define user acquisition procedures (unclassified, classified, terminal and mainframe system);

and submit implementation plans and procedures for client approval.